APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,936	08/27/2003	Richard A. Steinmetz	D-1150 DIV	5940

			EXAMINER
28995	7590	11/03/2006	HAMILTON, LALITA M

RALPH E. JOCKE
walker & jocke LPA
231 SOUTH BROADWAY
MEDINA, OH 44256

ART UNIT	PAPER NUMBER
3691	

DATE MAILED: 11/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/648,936
Filing Date: August 27, 2003
Appellant(s): STEINMETZ ET AL.

MAILED

NOV 0 3 2006

GROUP 3600

Ralph E. Jocke
<u>For Appellant</u>

EXAMINER'S ANSWER

This is in response to the appeal brief filed July 20, 2006 appealing from the Office

action mailed April 24, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Dulude October 30, 2001 US 6,310,966

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 13-24 and 28-34 are rejected under 35 U.S.C. 102(e) as being

anticipated by Dulude (6,310,966).

Dulude discloses biometric certificates for ATMs comprising a method and

corresponding computer readable media for receiving a certificate through operation of

the banking machine, authenticating at least one digital signature associated with the

certificate through operation of the banking machine, configuring the banking machine

responsive to the certificate and authentication of the at least one digital signature

(col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-

45); the certificate includes the digital signature, wherein the digital signature is

authenticated responsive to a public key of a licensing authority (col.1, line 65 to col.2,

line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); the certificate

corresponds to at least one software component authorized to be installed on the

banking machine, and further comprising installing the at least one software component

on the banking machine (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-

50; and col.8, lines 34-45); the certificate includes a plurality of sets of configuration

rules each set corresponding to at least one of a plurality of automated banking

machines, and wherein the banking machine is enabled to be configured responsive to

at least one set (col.10, lines 1-45); the certificate further includes an expiration

parameter, and further comprising determining through operation of the banking

machine responsive to the expiration parameter that configuration of the software on the

machine is not authorized and preventing configuration of software on the banking

machine responsive to the determination (col.1, line 65 to col.2, line 15); the certificate

includes an identification value unique to the banking machine (col.1, line 65 to col.2,

line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); determining

through operation of the banking machine that the identification value corresponds to a

hardware embedded identification value in the banking machine (col.1, line 65 to col.2,

line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); the certificate

includes a terminal identification value, including associating the machine with the

terminal identification value (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines

33-50; and col.8, lines 34-45); determining that the terminal identification value has

changed and preventing the machine from performing at least one transaction function

responsive to the determination (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5,

lines 33-50; and col.8, lines 34-45); retrieving the certificate from a licensing authority

(col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-

45); receiving the certificate from a server in operative connection with the banking

machine (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8,

lines 34-45); and computer readable media bearing instructions which are operative to

cause a computer in an automated banking machine to carry out the method steps of

receiving a certificate through operation of the banking machine, authenticating at least

one digital signature associated with the certificate through operation of the banking

machine, and configuring the banking machine responsive to the certificate and

authentication of the at least one digital signature (col.1, line 65 to col.2, line 15; col.3,

lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); receiving a certificate through

operation of the banking machine, authenticating at least one digital signature

associated with the certificate through operation of the banking machine, configuring the

banking machine responsive to the certificate and authentication of the at least one

digital signature (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and

col.8, lines 34-45); receiving at least one digitally signed certificate through operation of

the ATM, wherein the ATM includes a cash dispenser and at least one processor,

wherein the at least one certificate includes at least one serial number and verifying

through operation of the at least one processor that the at least one serial number

included in the at least one certificate corresponds to at least one serial number

associated with at least one hardware device of the ATM and responsive, configuring

the ATM through operation of the at least one processor responsive to the at least one

digital certificate (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and

col.8, lines 34-45); the at least one certificate includes at least one digital signature; and

further comprising authenticating the at least one digital signature through operation of

the at least one processor (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines

33-50; and col.8, lines 34-45); includes receiving the at least one certificate from a

server in operative connection with the ATM through a network (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); the at least one hardware device corresponds to at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device, wherein in configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); the at least one transaction function includes dispensing cash, wherein further comprising dispensing cash from the ATM through operation of the cash dispenser (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45); and configuring the ATM responsive to at least one key provided in the at least one certificate (col.1, line 65 to col.2, line 15; col.3, lines 28-50; col.5, lines 33-50; and col.8, lines 34-45).

(10) Response to Argument

With regard to independent claim 13, the Appellant argues that Dulude does not disclose:

a) receiving a certificate through operation of the banking machine;

b) authenticating at least one digital signature associated with the certificate through operation of the banking machine;

c) configuring the banking machine responsive to the certificate and

authentication of the at least one digital signature in step (b).

In response, Dulude discloses:

a) receiving a certificate through operation of the banking machine (the ATM

receives the certificate via a smart card—col.5, lines 33-50);

b) authenticating at least one digital signature associated with the certificate

through operation of the banking machine (a digital signature is generated to

form the biometric certificate (col.4, lines 10-25), and the ATM referred to in col.5,

lines 33-50 is used to receive the certificate via a smart card, thus authenticating

at least one digital signature associated with the certificate through operation of

the banking machine);

c) configuring the banking machine responsive to the certificate and

authentication of the at least one digital signature in step (b) (a digital signature is

generated to form the biometric certificate (col.4, lines 10-25), and the ATM

referred to in col.5, lines 33-50 is used to receive the certificate via a smart card,

thus authenticating at least one digital signature associated with the certificate

through operation of the banking machine).

With regard to claim 14, the Appellant argues that Dulude does not disclose

authenticating a digital signature included in a certificate or a digital signature that is

authenticated responsive to a public key of a licensing authority.

In response, Dulude discloses authenticating a digital signature included in a

certificate a digital signature is generated to form the biometric certificate (col.4, lines

10-25), and the ATM referred to in col.5, lines 33-50 is used to receive the certificate via a smart card) and a digital signature that is authenticated responsive to a public key of a licensing authority (the digital signature is generated using biometric certificates from a set of data—col.4, lines 5-12---the biometric certificate may be generated by processing the registration biometric data and processing the public key of the user at a biometric certificate generator of a registration authority (col.4, lines 55-65).

With regard to claim 15, the Appellant argues that Dulude does not disclose wherein the certificate corresponds to at least one software component authorized to be installed on the banking machine, and further comprising installing the at least one software component on the banking machine.

In response, Dulude discloses wherein the certificate corresponds to at least one software component authorized to be installed on the banking machine (the digital certificate is installed on the smart card, and the ATM is used to receive the digital certificate via the smart card—col.4, lines 10-25 and col.5, lines 33-50), and further comprising installing the at least one software component on the banking machine (the smart card may pre-store the biometric certificates, such that kiosks and other devices such as terminals and automated teller machines (ATMs) may access the memory and obtain the secured biometric certificate of the first user (col.5, lines 45-50).

With regard to claim 16, the Appellant argues that Dulude does not disclose the certificate includes a plurality of sets of configuration rules each set corresponding to at least one of a plurality of automated banking machines, and wherein the banking machine is enabled to be configured responsive to at least one set.

In response, Dulude discloses a certificate includes a plurality of sets of configuration rules each set corresponding to at least one of a plurality of automated banking machines, and wherein the banking machine is enabled to be configured responsive to at least one set (the certificate is stored on the smart card and has rules that allow it to be used in kiosks and other devices such as terminals and automated teller machines (ATMs)—col.5, lines 40-50).

With regard to claim 17, the Appellant argues that Dulude does not disclose wherein the certificate further includes an expiration parameter, and further comprising determining through operation of the banking machine responsive to the expiration parameter that configuration of the software on the machine is not authorized, and preventing configuration of software on the banking machine responsive to the determination.

In response, Dulude discloses wherein the certificate further includes an expiration parameter, and further comprising determining through operation of the banking machine responsive to the expiration parameter that configuration of the software on the machine is not authorized, and preventing configuration of software on the banking machine responsive to the determination (authenticating certificates may be generated with a validity period to determine an expiration of the validity of the certificate (col.1, line 65 to col.2, line 13).

With regard to claim 18, the Appellant argues that Dulude does not disclose wherein the certificate includes an identification value unique to the banking machine.

In response, Dulude discloses the certificate includes an identification value unique to the banking machine (the authenticating certificates may include identifying information and other data extensions indicating privileges and attributes of the certificate, such as access privileges (col.1, line 65 to col.2, line 15).

With regard to claim 19, the Appellant argues that Dulude does not disclose determining through operation of the banking machine that the identification value corresponds to a hardware embedded identification value in the banking machine.

In response, Dulude discloses determining through operation of the banking machine that the identification value corresponds to a hardware embedded identification value in the banking machine (the authenticating certificates may include identifying information and other data extensions indicating privileges and attributes of the certificate, such as access privileges (col.1, line 65 to col.2, line 15).

With regard to claim 20, the Appellant argues that Dulude does not disclose wherein the certificate includes a terminal identification value, and associating the machine with the terminal identification value.

In response, Dulude discloses wherein the certificate includes a terminal identification value, and associating the machine with the terminal identification value (the authenticating certificates may include identifying information and other data extensions indicating privileges and attributes of the certificate, such as access privileges (col.1, line 65 to col.2, line 15).

With regard to claim 21, the Appellant argues that Dulude does not disclose determining that the terminal identification value has changed and preventing the

machine from performing at least one transaction function responsive to the determination.

In response, Dulude discloses determining that the terminal identification value has changed and preventing the machine from performing at least one transaction function responsive to the determination (the authenticating certificates may include identifying information and other data extensions indicating privileges and attributes of the certificate, such as access privileges (col.1, line 65 to col.2, line 15).

With regard to claim 22, the Appellant argues that Dulude does not disclose retrieving the certificate from a licensing authority.

In response, Dulude discloses retrieving the certificate from a licensing authority (the biometric certificate is retrieved and sent to the biometric certificate extractor to decrypt the biometric certificate using the public key of the certifying authority (col.6, lines 58-65).

With regard to claim 23, the Appellant argues that Dulude does not disclose receiving the certificate from a server in operative connection with the banking machine.

In response, Dulude discloses receiving the certificate from a server in operative connection with the banking machine (the certificate is received via the smart card in operative connection with the banking machine—col.5, lines 40-50).

With regard to claim 24, the Appellant argues that Dulude does not disclose computer-readable media bearing instructions which are operative to cause a computer in an automated banking machine to carry out the method steps of:

a) receiving a certificate through operation of the banking machine;

b) authenticating at least one digital signature associated with the certificate

through operation of the banking machine;

c) configuring the banking machine responsive to the certificate and

authentication of the at least one digital signature in step (b).

In response, Dulude discloses computer-readable media bearing instructions

which are operative to cause a computer in an automated banking machine to

carry out the method steps of:

a) receiving a certificate through operation of the banking machine (the ATM

receives the certificate via a smart card—col.5, lines 33-50);

b) authenticating at least one digital signature associated with the certificate

through operation of the banking machine (a digital signature is generated to

form the biometric certificate (col.4, lines 10-25), and the ATM referred to in col.5,

lines 33-50 is used to receive the certificate via a smart card, thus authenticating

at least one digital signature associated with the certificate through operation of

the banking machine);

c) configuring the banking machine responsive to the certificate and

authentication of the at least one digital signature in step (b) (a digital signature is

generated to form the biometric certificate (col.4, lines 10-25), and the ATM

referred to in col.5, lines 33-50 is used to receive the certificate via a smart card,

thus authenticating at least one digital signature associated with the certificate

through operation of the banking machine).

With regard to claim 28, the Appellant argues that Dulude does not disclose

a method for configuring a cash dispensing automated teller machine (ATM) comprising:

a) receiving at least one digitally signed certificate through operation of the ATM, wherein the ATM includes a cash dispenser and at least one processor, wherein the at least one certificate includes at least one serial number

b) verifying through operation of the at least one processor that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM;

c) responsive to (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate.

In response, Dulude discloses a method for configuring a cash dispensing automated teller machine (ATM) comprising:

a) receiving at least one digitally signed certificate through operation of the ATM, wherein the ATM includes a cash dispenser and at least one processor, wherein the at least one certificate includes at least one serial number (the ATM receives the certificate via a smart card—col.5, lines 33-50---and authenticating certificates include a serial number—col.2, lines 1-10);

b) verifying through operation of the at least one processor that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM (authenticating certificates include a serial number and other data extensions indicating privileges and attributes of the certificate, such as access privileges--

col.2 lines 1-10—which may indicate which devices may have access to the

authenticating certificates contained on the smart card that is used in the ATM—

col.5, lines 40-50);

c) responsive to (b), configuring the ATM through operation of the at least one

processor responsive to the at least one digital certificate (the ATM receives the

certificate via a smart card—col.5, lines 33-50).

With regard to claim 29, the Appellant argues that Dulude does not disclose the

at least one certificate includes at least one digital signature; and further comprising:

authenticating the at least one digital signature through operation of the at least one

processor.

In response, Dulude discloses at least one certificate includes at least one digital

signature; and further comprising: authenticating the at least one digital signature

through operation of the at least one processor (col.4, lines 10-25), and the ATM

referred to in col.5, lines 33-50 is used to receive the certificate via a smart card) and a

digital signature that is authenticated responsive to a public key of a licensing authority

(the digital signature is generated using biometric certificates from a set of data—col.4,

lines 5-12---the biometric certificate may be generated by processing the registration

biometric data and processing the public key of the user at a biometric certificate

generator of a registration authority (col.4, lines 55-65).

With regard to claim 30, the Appellant argues that Dulude does not disclose

receiving the at least one certificate from a server in operative connection with the ATM

through a network.

In response, Dulude discloses receiving the at least one certificate from a server in operative connection with the ATM through a network (the ATM receives the certificate via a smart card—col.5, lines 33-50).

With regard to claim 31, the Appellant argues that Dulude does not disclose wherein the at least one hardware device corresponds to at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device.

In response, Dulude discloses wherein the at least one hardware device corresponds to at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device (the ATM receives the certificate via a smart card through a card reader—col.5, lines 33-50).

With regard to claim 32, the Appellant argues that Dulude does not disclose wherein the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device, wherein in configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device.

In response, Dulude discloses wherein the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device, wherein in configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device (authenticating certificates may be generated with a validity period to determine an expiration of the validity of the certificate--col.1, line 65 to col.2, line 13—if certificate is still valid, then it may be used, if not valid, then it will not be able to be used).

With regard to claim 33, the Appellant argues that Dulude does not disclose wherein the at least one transaction function includes dispensing cash, wherein further comprising: dispensing cash from the ATM through operation of the cash dispenser.

In response, Dulude discloses the at least one transaction function includes dispensing cash, wherein further comprising: dispensing cash from the ATM through operation of the cash dispenser (the user will go to the ATM to retrieve funds made through electronic funds transfers—col.5, lines 50-62).

With regard to claim 34, the Appellant argues that Dulude does not disclose configuring the ATM responsive to at least one key provided in the at least one certificate.

In response, Dulude discloses configuring the ATM responsive to at least one key provided in the at least one certificate (the digital signature is generated using biometric certificates from a set of data—col.4, lines 5-12---the biometric certificate may be generated by processing the registration biometric data and processing the public key of the user at a biometric certificate generator of a registration authority (col.4, lines 55-65).
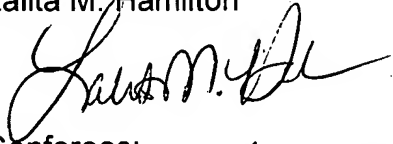
(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Lalita M. Hamilton

Conferees:

Vincent Millin

Alexander Kalinowski